



## PIER Energy System Integration Program Area

### Enterprise Infrastructure Security - Target 86

**Contract #:** 500-00-023 **Project #:** 15

**Contractor:** Electric Power Research Institute (EPRI)

**Project Amount:** \$45,000

**Match Amount:** \$1,209,615

**Contractor Project Manager:** Jim Fortune (650) 855-2500

**Commission Contract Manager:** Laurie ten Hope (916) 654-4637

**Status:** Completed

#### Project Description:

The purpose of this project is to address concerns over the security of the energy industry's electronic infrastructure against cyber and physical threats. These threats range from corporate espionage by competitive rivals to sabotage by hackers or terrorists. Immediate concerns center on the vulnerabilities of electronic operations systems such as supervisory control and data acquisition (SCADA) and plant distributed control systems (DCS) and their interconnectivity with corporate business systems. As the energy industry becomes increasingly automated and electronically connected, a concerted cyber attack could be catastrophic from business, customer and national security perspectives. This project identifies and addresses security issues through a series of working group meetings that include staff and managers from the Energy Commission and other agencies, with the ultimate goal of developing more robust electronic security programs. Meetings and workshops provide forums for sharing information on best practices, lessons learned, and vulnerability assessment results.

#### This project supports the PIER Program goal of:

- Improving the reliability of California's electricity by leveraging the collective knowledge of the participants to develop strategies for protecting the state's critical electric power infrastructure against cyber and physical threats.

#### Proposed Outcomes:

1. Organize and facilitate workshops for collaborative exchange of information and ideas to support the development of robust security programs.
2. Provide guidelines, policies and procedures reflecting the collective knowledge of the industry for the following activities:
  - Specifying equipment procurement.
  - Performing tradeoffs between equipment performance and security.
  - Interfacing between information technology (IT) and operating systems.
3. Enhance the dedicated EIS website with expanded content to provide more and higher value information.
4. Engage key operating systems vendors and collaboratively develop security-based functional specifications for new hardware and software.
5. Develop a risk assessment framework to help decision makers understand and evaluate the costs and benefits of different security measures.

**Actual Outcomes:**

1. Workshops – Four topical workshops were delivered in 2001.
2. Guidelines, Policies and Procedures – The following technical reports were published in 2001 and are available on the members-only EIS web site:
  - Equipment Procurement Guidelines.
  - Performance/Security Tradeoff Guidelines.
  - Interfacing IT and Operations Systems Guidelines.
  - Generic Policies and Procedures.
3. Website.
  - The EIS member website was expanded.
4. Security-Based Specifications.
  - A technical report was published that describes generic specifications for operating system software and hardware resulting from the collaborative efforts of vendor action groups.
5. Risk Assessment Framework.
  - A web-accessible risk assessment framework was developed.

**Project status:**

The project has been completed.